CLAIMS

What is claimed is:

1. A communication switch comprising:

at least one input for receiving messages, each message including,

an address specifier, and

a port specifier;

a traffic analyzer for comparing the port specifier of a first message against the port specifiers of previously received messages; and

an output for reporting a result of the comparing.

2. The communication switch of claim 1 further comprising:

a usage tracking system for throttling traffic through the communication switch.

3. The communication switch of claim 2 wherein:

the usage tracking system includes means for throttling traffic according to address specifier and port specifier in combination.

4. The communication switch of claim 2 wherein:

the usage tracking system includes means for throttling traffic according to a predetermined maximum aggregate bandwidth for the communication switch.

5. The communication switch of claim 1 wherein:

the traffic analyzer is further for reporting fraud over the output.

6. The communication switch of claim 1 wherein:

the traffic analyzer is further for comparing the address specifier and port specifier combination of the first message against the address specifier and port specifier combinations of the previously seen messages.

7. The communication switch of claim 1 wherein:

each message further includes,

a traffic type specifier; and

the traffic analyzer is further for comparing the traffic type specifier of the first message against the traffic type specifiers of the previously received messages.

8. The communication switch of claim 1 wherein:

each message further includes,

a traffic type specifier; and

the traffic analyzer is further for comparing the address specifier, port specifier, and traffic type specifier of the first message against the address specifier, port specifier, and traffic type specifier combinations of the previously received messages.

9. A server for use with a communication switch, the server comprising:

an I/O for communicating messages and alerts between the communication switch and the server;

a billing system for providing a maximum bandwidth indication to the communication switch; and

a fraud detection system for receiving fraud alerts from the communication switch.

10. The server of claim 9 wherein:

the fraud detection system is responsive to fraud alerts indicating excessive traffic on an address:port combination at the communication switch.

11. The server of claim 10 wherein:

the fraud detection system is further responsive to fraud alerts indicating a likelihood of IP masquerading.

12. The server of claim 10 wherein:

the fraud detection system is responsive to fraud alerts based upon address:port:type combination.

13. A method comprising:

receiving a message which includes an address:port identifier;

comparing the address:port identifier against previously received messages' address:port identifiers; and

determining whether excessive traffic is originating from a source identified by the address:port identifier.

14. The method of claim 13 further comprising:

throttling message traffic in response to determining that excessive traffic is originating from the source.

15. The method of claim 14 wherein the throttling comprises:

throttling message traffic to and/or from that source.

16. The method of claim 13 wherein the message further includes a type specifier, the method further comprising:

comparing the type specifier against type specifiers of previously received messages from the same address:port as the message; and

determining whether the source is issuing messages of different types such as indicate fraud.

17. The method of claim 16 further comprising:

sending a fraud alert in response to determining that the source is issuing messages of different types such as indicate fraud.

18. The method of claim 13 further comprising:

recording the message for use in future comparisons against future messages.

19. The method of claim 13 further comprising:

receiving an indication of a maximum bandwidth; and

throttling message traffic in response to the indication of the maximum bandwidth.

20. A customer premises gateway for communicating with an ISP premises head-end server, the customer premises gateway comprising:

at least one first I/O each for connecting to a communication device;

a second I/O for connecting to the ISP premises head-end server; and

a traffic analyzer coupled to the at least one first I/O and the second I/O, including

a port identifier comparator,

a throttling mechanism, and

a fraud reporter.

21. The customer premises gateway of claim 20 wherein the traffic analyzer further includes:

a message type analyzer.

22. A machine accessible medium including therein instructions which, when executed by the machine, cause the machine to:

compare a first address:port combination of a message against a second address:port combination of a previously received message; and

responsive to the address:port comparison, determine whether excessive traffic is going to/from the first address:port combination.

23. The machine accessible medium of claim 22 further including therein instructions which, when executed by the machine, cause the machine to further:

throttle traffic to/from the first address:port combination.

24. The machine accessible medium of claim 23 further including therein instructions which, when executed by the machine, cause the machine to further:

report fraud.

25. The machine accessible medium of claim 22 further including therein instructions which, when executed by the machine, cause the machine to further:

compare a first type specifier of the message against a second type specifier of the previously received message; and

responsive to the type specifier comparison, determine whether the first address:port identifies a router performing address:port masquerading.

26. The machine accessible medium of claim 25 further including therein instructions which, when executed by the machine, cause the machine to further:

report the masquerading.

27. A method for a communication switch to detect that a device connected to the communication switch is a router, comprising:

receiving from the device a message including address and sub-address identifiers;

comparing the address and sub-address identifiers against one or more previously received messages; and

detecting that the address and sub-address identifiers indicate that the device is performing masquerading.

28. The method of claim 27 wherein the detecting comprises:

observing a first message type indicator in the message and a different message type indicator in at least one of the previously received messages.

29. The method of claim 27 further comprising:

recording the address and sub-address identifiers of the message;

receiving a second message; and

comparing the second message's address and sub-address identifiers against the recorded address and sub-address identifiers.

30. The method of claim 27 wherein:

the address identifier comprises an Internet Protocol address; and

the sub-address identifier comprises a port number.

31. The method of claim 27 further comprising:

responsive to detecting masquerading, sending a fraud alert to a server.

32. The method of claim 27 further comprising:

throttling message transmission.

33. The method of claim 27 further comprising:

comparing a message type identifier of the message against one or more previously received messages; and

detecting that the message type identifier of the message is different than a message type identifier of a previously received message having a same address identifier and a same sub-address identifier as the message.

34. The method of claim 33 wherein:

the address identifier comprises an Internet Protocol address;

the sub-address identifier comprises a port number; and

the message type identifier comprises one of an HTTP specifier and an FTP specifier.